WILMERHALE

Department of Commerce Now Accepting Privacy Shield Self-Certifications: A Primer for Compliance and Self-Certification

AUGUST 2, 2016

The Privacy Shield framework is a voluntary program that provides companies with a mechanism for complying with EU data protection requirements when transferring personal data from the EU to the US. The framework is open to businesses subject to the enforcement jurisdiction of the US Federal Trade Commission or the US Department of Transportation. It replaces the Safe Harbor program and has a number of substantive new requirements that should be considered before a company self-certifies under the framework, including:

- **An Expanded Privacy Notice:** The Privacy Shield notice requirements are more specific and detailed than under the Safe Harbor program, and an enrollee's public privacy policy must provide additional information about a company's data practices and participation in the Privacy Shield.
- **New Contract Requirements with Third-Parties and Vendors:** Onward data transfers will require written contractual agreements, and enrollees now bear the burden to demonstrate that they are not responsible and liable for any damages that results from processing by third parties. However, in order to encourage companies to join, the Privacy Shield offers companies that self-certify by October a nine-month period to bring their existing commercial relationships into compliance.
- **Regulatory Oversight Requirements:** The US Department of Commerce will be conducting compliance reviews of companies in the Privacy Shield framework, which may include detailed questionnaires and other information requests. Enrollees must agree to respond promptly to inquiries and request for documentation about their Privacy Shield compliance.
- **New Redress Mechanisms for EU Data Subjects:** To address perceived difficulties resolving individual complaints under Safe Harbor, the Privacy Shield envisions several different redress mechanisms. Enrollees must have procedures in place to address individual complaints and must respond to an individual within 45 days. They must also offer an alternative dispute resolution provider free of charge. EU Data Subjects may complain to their home data protection authority and can invoke binding arbitration for some residual claims not resolved by other redress mechanisms.
- **Potential Additions in the Future:** The Privacy Shield is also designed to be updated over time, both to address new issues and to accommodate the General Data Protection

Regulation when it goes into effect in 2018. The European Commission and US Department of Commerce have agreed to discuss potential rules around automated processing at the Privacy Shield's first annual review.

Except for a grace period around third-party contract compliance, the Privacy Shield's requirements apply immediately upon an enrollee's certification with the US Department of Commerce. Before self-certifying, a company will need to do the following:

- **Confirm Eligibility to Participate:** Only companies that are subject to the enforcement jurisdiction of the Federal Trade Commission or the Department of Transportation may join the Privacy Shield framework.
- **Identify and Register with an Independent Recourse Mechanism:** An enrollee must ensure that its recourse mechanism is in place prior to self-certification and, if required, must register with that organization prior to self-certification.
- **Ensure Verification Mechanisms Are in Place:** Enrollees must put in place procedures either via self-assessment or through third-party assessment programs to verify their continuing compliance with the Privacy Shield's requirements.
- **Designate a Privacy Shield Point-of-Contact:** Enrollees must designate a contact person responsible for the company's privacy compliance to handle questions, complaints, access requests, and any other issue arising under the Privacy Shield.
- **Provide Detailed Information to the US Department of Commerce:** The Department of Commerce has provided a detailed list of information that must be verified before a company may join the Privacy Shield. Enrollees will need to provide contact information, describe their activities with respect to personal information received from the European Union, and identify what personal information is covered by its self-certification.

Pre-Certification Checklist

According to the European Commission, the combination of mechanisms and procedures provided by the Privacy Shield approximate the requirements of the EU Data Protection Directive. The foundation of the framework is that companies are required to publicly commit to follow the seven Privacy Shield principles (which also include 16 supplemental principles). The Privacy Shield principles are:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement, and Liability

The seven principles (and associated supplemental principles) are discussed beginning on page sixteen of the Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-

US Privacy Shield (available here: http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf). The supplemental principles expand upon information provided in Frequently Asked Questions to the invalidated Safe Harbor regime (available here, beginning at 15: http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf), and are now formally incorporated into the Privacy Shield framework.

The following are steps that you should consider before self-certifying under the Privacy Shield framework. While the Department of Commerce has provided an online guide to self-certification (available here: https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/how_to_join_privacy_shield_sc_cmts.pdf) this document should help you to identify items, practices, and procedures that will require attention as you prepare to self-certify. Privacy Shield is a voluntary framework, but self-certification constitutes a legal commitment to comply with the program and may be enforced by the Federal Trade Commission and the Department of Transportation.

Privacy Officer: You should designate a person to be responsible for coordinating Privacy Shield compliance. Often, that person is either the Human Resources manager or the person responsible for the company's privacy practices in general. This person should be the single point of contact for all Privacy Shield issues. The Privacy Shield framework requires that a contact be provided to handle any questions, complaints, or access requests that may arise under the Privacy Shield.

Internal Assessments: You should conduct an assessment of the data practices for which Privacy Shield self-certification is being considered. You should identify what information will be (and is already being) collected from EU data subjects and how it will be used and/or disclosed. A self-certification need not apply to all EU personal data maintained by your company but must specify to which data it does apply. Self-certification may be limited to online data, offline data, human resources data, or any combination from among these categories.

If a company self-certifies for human resources data for use in employment, it must take additional steps:

- Indicate that it is extending Privacy Shield benefits to human resources data when it self-certifies.
- Commit to cooperate and comply with data privacy authorities to resolve complaints concerning its use of such data.
- Provide the Department of Commerce with a copy of its human resources privacy policy.
- Make the privacy policy available for viewing by affected employees.

You may continue to rely on model contractual clauses for data that you choose to exclude from your Privacy Shield certification.

Privacy Policy/Notice: You should use the internal assessment to prepare a narrative policy statement that describes how your practices conform to the Privacy Shield principles. If you have an existing privacy policy, it likely can be adapted through the addition of a new section discussing the Privacy Shield framework. By the time the self-certification is completed, your Notice should provide information about:

- A statement that your policy adheres to the Privacy Shield Principles, a hyperlink to the Privacy Shield website (https://www.privacyshield.gov), any entities or subsidiaries of the organization also adhering to the Privacy Principals, and a commitment that the Privacy Shield principles will apply to all personal data received from the EU in reliance on the Privacy Shield.
- The types of personal data collected and the purpose for which it is collected.
- How to contact you with any inquiries or complaints.
- The types or identify of third parties to which you disclose personal data, and the purposes for which you do so.
- The right of individuals to access their personal data and the choices and means you offer individuals for limiting the use and disclosure of their personal data.
- The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, whether that body is established by data protection authorities, whether that body is based in the EU or the United States, and a hyperlink to the dispute resolution body.
- That the organization is subject to the investigatory and enforcement powers of the FTC, Department of Transportation, or another US authorized statutory body.
- The possibility, under certain conditions, for the individual to invoke binding arbitration.
- The requirement to disclose personal data in response to lawful requests by public authorities.
- Your potential liability in cases of transfers to third parties.

The policy must be posted on a public web site (subject to narrow exceptions, such as if your certification relates only to human resources data) and it must be submitted to the US Department of Commerce's Privacy Shield team for formal review.

Opt In/Opt Out Choices: If any data subject to the self-certification will be disclosed to non-agent third parties (see below) or used for a materially different purpose than that for which it was collected, there must be procedures for allowing individual data subjects to "opt out" from such uses or disclosures. If any secondary uses or third-party disclosures involve "sensitive" data (i.e., personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, or criminal history), there must be procedures ensuring that data subjects affirmatively "opt in" prior to such use or disclosure.

Contracts with Third Parties for Onward Data Transfers: You must identify all third parties (or, at least, the types of third parties) receiving access to the data that will be subject to the self-certification, and you must determine whether they will be acting "as agents to perform task(s) on behalf of and under the instructions of the [self-certifying] organization."

The Privacy Shield guidance is not clear, but one should not assume that "agents" for Privacy Shield purposes are always "agents" within the traditional legal meaning of that term; however, contractors performing under your instructions may generally be considered agents for purposes of the Accountability for Onward Transfer principle.

For third parties acting as agents, you must:

- Transfer personal data only for limited and specified purposes.
- Ascertain that the agent is required to provide the same level of protection as the Privacy Shield principles (you should do due diligence, especially as to the Accountability for Onward Transfer, Security, and Data Integrity and Purpose Limitation requirements; the Notice, Access, Choice, and Recourse, Enforcement, and Liability principles may not always be applicable to a third party that does not interact directly with data subjects).
- Take steps to ensure that the agent effectively processes personal data consistent with the organization's Privacy Shield obligations.
- Require the agent to notify the organization if the agent can no longer meet its obligations.
- Upon such notice, take steps to stop and remediate unauthorized processing.
- Provide information about relevant contractual provisions to the Department of Commerce upon request.

You must enter into a contract with each agent ensuring compliance with these obligations. Where a third-party agent violates the Privacy Shield principles, the Privacy Shield places the obligation on certified organizations to prove that they are not responsible for the event giving rise to the damage.

For third parties acting as data controllers, the Privacy Shield's notice and choice principles apply, requiring an opt-in or opt-out depending upon the use or type of data. You must also contract with each of these third parties, obliging them to:

- Process data only for limited and specified purposes consistent with the consent provided by the individual.
- Provide the same level of protection as the Privacy Shield principles.
- Notify you if it cannot meet its obligations and then cease processing or take other steps to remediate.

If a third party is engaged to perform clearly defined tasks, these requirements may be satisfied with an appropriately restrictive "data protection" clause that limits the recipient's use of data to the specific tasks, limits retention of data to the period of performance, prohibits any modifications or disclosures of data, requires industry-standard data security measures, and forbids any contact with data subjects. The data protection clause can be inserted into or appended to the service agreement under which the third party will work. Because these requirements will likely require new contractual agreements, the Privacy Shield incentivizes companies to self-certify by October 2016 by granting them a nine-month period to bring their existing commercial relationships into compliance. After that point, contracts with third parties for onward transfer must be in place before self-certifying.

Access Rights: Access to one's information is one of the fundamental elements of the Privacy Shield program, but this right of access is not absolute. Access can be restricted where the burden or expense of providing access would be disproportionate to the risk to the individual's privacy in the case in question, or where the rights of other persons would be violated. An internal policy or procedure should establish objective standards for determining whether and how access must be

provided, taking into account the specific needs and characteristics of your company and the anticipated expectations of the data subjects. Individuals have the right to obtain confirmation as to whether you hold personal data about them. Reasonable fees may be charged to defray the costs of providing access, but these fees (or limits on the number of times that a person may obtain access) should be specified in advance in to avoid a claim of discrimination. At a minimum, access must be provided in accordance with the requirements of Supplemental Principle 8 – Access (available here, beginning at 31: http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf). Amendment, correction, and deletion rights must be provided in where personal data—including accurate data—has been processed in violation of the framework.

Security Measures: You must implement reasonable measures to protect personal data from loss or unauthorized access, use, disclosure, alteration, or destruction. These measures should be documented and take into account the risks involved in the processing and the nature of the personal data.

Data Integrity Measures and Purpose Limitations: You must implement procedures to maximize the integrity of stored data, including taking reasonable steps to:

- Consider and approve requested amendments.
- Make unilateral amendments.
- Identify inaccurate, incomplete, or out-of-date information.

The Privacy Shield also requires that collection of personal data be "limited" to that which is "relevant for the purposes of processing," and organizations may not process information in ways "incompatible with the purpose for which it has been collected or subsequently authorized by the individual." "Compatible processing purposes" depend on circumstances, but could include those "that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection." The data should be retained only so long as it serves an original or compatible purpose for processing (although data may be retained indefinitely if it is not in a form "identifying or making identifiable the individual").

Recourse Mechanisms: Self-certifying companies must have in place procedures to respond to any individual complaints and must be able to respond to the merits of a complaint within forty-five days of receiving it. Additionally, you also must provide, at no cost to the individual, an independent recourse mechanism to resolve disputes arising in connection with a data transfer or subsequent use or disclosure of personal data. Private dispute resolution organizations—such as TRUSTe, the Council of Better Business Bureaus (BBB), the American Arbitration Association (AAA), JAMS, and the Direct Marketing Association (DMA)—may be used. Alternatively, you may choose to use EU Data Protection Authorities for this purpose, and companies are required to cooperate and comply with these authorities if their self-certification covers human resources data. (European officials have encouraged companies to opt for using EU Data Protection Authorities as their chosen avenue for resolving Privacy Shield complaints due to EU data subjects' familiarity with them. If your organization chooses to do so, you must comply with the additional requirements of Supplemental

Principle 5, available at https://www.privacyshield.gov/article?id=5-The-Role-of-the-Data-Protection-Authorities-a-b). If the recourse mechanism requires registration, you must do so prior to self-certification.

Employee Training: You should put in place training for employees who handle personal data from the EU. Staff familiar with your EU privacy policy can conduct the training in-house.

Changes in Data Practices: Changes in data practices may cause a company to become non-compliant with its Privacy Shield commitments. Before self-certifying, you should implement an internal procedure for ensuring that the designated Privacy Officer is informed well in advance of any proposed changes in the collection, use, or disclosure of data described in the Privacy Notice, so that appropriate modifications can be made to the Notice, internal procedures, or employee training program (or, where appropriate, so that proposed changes can be reviewed before implementation).

Verification Measures: Privacy Shield enrollees must audit and verify their compliance with the Privacy Shield principles. Prior to self-certifying, you should decide whether to rely upon an internal self-assessment or an outside, third-party program. An internal verification process must objectively check and document that:

- The Privacy Notice is accurate, comprehensive, prominently displayed, completely implemented, and accessible.
- Your practices comply with the Privacy Shield principles.
- Individuals are informed of available complaint processes including in-house arrangements and independent recourse mechanisms.
- Employees are adequately trained and disciplined, as appropriate.
- Procedures are in place for periodic compliance reviews.

A statement verifying a self-assessment must be signed by an appropriate company official at least once a year and made available upon request by individuals or regulators. Internal verification is not a “free pass”; there must be a legitimate, documented compliance assessment. Third-party verification programs (e.g., TRUSTe, etc.) have their own procedures and enrollment requirements, which should be reviewed before self-certifying.

Records Retention: You must have a records retention policy. Records pertaining to Privacy Shield certification and compliance should normally be maintained for at least five years.

Final Verification: You must make sure the Privacy Notice is effective and accurate, and make any necessary refinements before self-certifying. The location of the posted Privacy Notice (e.g., a specific public web site URL) will need to be provided on the self-certification form.

Annual Self-Certification: The US Department of Commerce has begun accepting self-certifications to the Privacy Shield on August 1, 2016, and has set up a Privacy Shield Website. See also Supplemental Principle 6 – Self-Certification (available here, beginning at Page 27: http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf) for a complete list of information that must be verified. After self-certifying, you must reaffirm this self-

certification annually. The reaffirmation submission must be made on or before the anniversary of the day on which your original self-certification was finalized. Before filing your reaffirmation, you must conduct an audit to confirm that you continue to comply with the Privacy Shield principles.

Ongoing Obligations: The new framework explicitly states that, even if an organization terminates its certification in Privacy Shield, the organization remains bound by the Privacy Shield principles with respect to any personal data it retains that was collected under the Privacy Shield. Organizations must continue to affirm their commitment to apply the principles to any retained data.

Administrative Fees: The US Department of Commerce plans to charge an annual contribution for self-certification to cover the cost of the Privacy Shield arbitration panel, and will identify the amount of that fee by January 2017. It is not yet clear whether the Department will impose other registration fees associated with administering the program. The Department's privacy shield team will be conducting industry briefings to provide more information about the process.

Self-certified organizations that agree to cooperate with EU data protection authorities (including all organizations certifying with respect to human resources data) will be required to pay an annual administrative fee of no more than $500 per year to defray the EU authorities' costs.